



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007*

April 4, 2019

BY ECF

The Honorable Jesse M. Furman
United States District Judge
Southern District of New York
40 Foley Square
Thurgood Marshall U.S. Courthouse
New York, New York 10007

Re: *United States v. Gary Davis, a/k/a "Libertas,"* 13 Cr. 950 (JMF)

Dear Judge Furman:

The Government respectfully submits this letter in advance of sentencing in the above-captioned case. In October 2018, defendant Gary Davis (the "defendant") pled guilty, pursuant to a plea agreement with the Government (the "Plea Agreement"), to conspiracy to distribute narcotics, stemming from his role in helping administer the Silk Road website. As noted in the Probation Office's final Presentence Investigation Report, the United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.") range applicable to this defendant is 168 to 210 months' imprisonment. For the reasons set forth below, the Government respectfully submits that a sentence within that range would be fair and appropriate in this case.

I. Offense Conduct

A. Overview

From January 2011 until October 2, 2013, the "Silk Road" website hosted a sprawling black-market bazaar on the Internet, where illegal drugs and other illicit goods and services were regularly bought and sold by the site's users. Silk Road was an online black market of unprecedented scope. By the time it was shuttered in October 2013, over 13,000 offerings were listed on its homepage for illegal drugs of virtually every variety. A wide variety of other illicit goods and services were sold on the site as well, including fake IDs and passports, computer-hacking tools and services, counterfeit goods and pirated media, criminal guidebooks and instruction manuals, and money laundering services. In total, over 1.5 million transactions were conducted over Silk Road, involving over 100,000 buyer accounts and nearly 4,000 seller accounts. Those transactions had a total value of more than \$213 million in U.S. currency. Nearly 95 percent of those sales (approximately \$183 million worth) were for illegal drugs—including at least \$8.9 million in sales of heroin, \$17.3 million in sales of cocaine, and \$8.1 million in sales of methamphetamine. The buyers and sellers involved in these transactions were spread across the world. (See Final Presentence Investigation Report dated February 22, 2019 ("PSR"), ¶¶ 14–15, 42; see also Dkt. 35 (Gov't Sentencing Letter as to Nash)).

Hon. Jesse M. Furman
United States District Judge

Page 2
April 4, 2019

The owner and operator of Silk Road, Ross William Ulbricht, a/k/a “Dread Pirate Roberts,” a/k/a “DPR,” a/k/a “Silk Road,” ran the website with the assistance of a small support staff. (PSR ¶ 16). At the time the site was taken down, that support staff consisted of four members.

From May 2013 up to June 2013, the defendant served as a “forum moderator” for Silk Road. Forum moderators were responsible for, among other things, monitoring user activity on discussion forums associated with the site, providing guidance to forum users concerning how to conduct business on Silk Road, and reporting any significant problems discussed on the forums to the site administrators and to Ulbricht. Then, from June 2013 until Silk Road was taken down by law enforcement in early October 2013, the defendant worked as a site administrator on Silk Road. In his role as a site administrator, the defendant’s responsibilities included (1) responding to customer support requests from Silk Road users who needed assistance with their buyer or seller accounts on the marketplace; (2) investigating disputes that arose between vendors (*e.g.*, drug dealers) and buyers, including reporting his findings to co-defendant Andrew Michael Jones or to Ulbricht; and (3) helping enforce the rules for doing business on Silk Road, which had been set by Ulbricht, including demoting a vendor or referring the vendor for further discipline. (*Id.* ¶¶ 16–17).

After law enforcement arrested Ulbricht and took down the Silk Road website, the defendant (and others) continued the same type of unlawful activity on “Silk Road 2.0,” as discussed in greater detail below. The defendant’s involvement in Silk Road 2.0 ended after approximately one month, due to his arrest in this case. (*Id.* ¶ 18).

B. Overview of the Silk Road Website

Silk Road was an extensive and sophisticated online criminal marketplace that sought to make conducting illegal transactions on the Internet as easy and frictionless as shopping online at mainstream e-commerce websites. The website offered a sales platform that allowed users of the website to conduct transactions online, and the basic user interface resembled those of well-known online marketplaces. (*Id.* ¶ 20).

1. The Tor Network

Unlike mainstream commerce websites, Silk Road was only accessible on the Tor network. The Tor network is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet protocol addresses (or “IP addresses”) of the computers on the network and, thereby, the identities of the network’s users. Although Tor has legitimate uses, it is also used by cybercriminals seeking to anonymize their computer. Every communication sent through Tor is bounced through relays within the network, and wrapped in layers of encryption, such that it is practically impossible to trace the communication back to its true originating IP address. (*Id.* ¶ 21).

Tor also allows websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, referred to as “hidden services.” Such “hidden services” operating on Tor have complex web addresses ending in “.onion.” Such addresses can only be accessed using special Tor web browser software. (*Id.* ¶ 22).

Hon. Jesse M. Furman
United States District Judge

Page 3
April 4, 2019

2. Silk Road User Interface

Upon arriving at the Silk Road website, a user was presented with a blank screen containing a prompt for a username and password. Users could create a new account simply by creating a unique username and password. No other information was required, such as information about the identity or age of the user. (*Id.* ¶ 23).

After a user entered a username and password, the user was then directed to Silk Road's homepage, which, in the upper left hand corner, contained the logo for the website, labeled "Silk Road anonymous market." On the left hand side of the screen, there was a list labeled "Shop by Category," containing links to various categories of illegal items for sale on the site, including most prominently, "Drugs," and various subcategories of types of illegal narcotics. The center of the homepage contained photographs of a sample of current listings on the website. *See* Ex. A. The homepage also included links which permitted users to access: (1) a private message system, which allowed users to send messages to each other through the website, similar to emails; (2) online forums where users could post messages to "discussion threads" concerning various topics related to the website; (3) a "wiki" which contained a collection of frequently asked questions, and other forms of guidance for users; and (4) a "customer service" section, where users could get support from the Silk Road administrative staff. (PSR ¶ 24).

When a user clicked on any of the links to items for sale, the website would bring up a page containing the details of the listing, including a description of the item, the price of the item, the username of the vendor selling it, and reviews of the product posted by previous customers. *See* Ex. B. To purchase an item, the user would simply click on a link to add the item to an electronic "shopping cart." The user would later be prompted to supply a shipping address and to confirm the placement of the order. Once the order was placed, it would be processed through Silk Road's Bitcoin-based payment system, described in detail below. (PSR ¶ 25).

3. Illegal Goods and Services Sold on the Silk Road Website

The illegal nature of the items sold on Silk Road was readily apparent to any user browsing through its offerings. (*Id.* ¶ 26). The illegal goods and services, included, among other things:

a. *Illegal Narcotics*

The vast majority of the goods for sale were illegal drugs of nearly every variety, which were openly advertised on the site as such and were immediately and prominently visible on the site's home page. As of the takedown of the Silk Road website on October 2, 2013, there were nearly 13,802 listings for controlled substances on the website, listed under the categories "Cannabis," "Dissociatives," "Ecstasy," "Intoxicants," "Opioids," "Precursors," "Prescription," "Psychedelics," and "Stimulants," among others. As of the same date, among other illegal narcotics, there were at least approximately 643 different listings for cocaine products, which included listings for cocaine base (commonly known as "crack" cocaine), 205 different listings for heroin products, at least 305 different listings for LSD products, and 261 different listings for methamphetamine products. (*Id.* ¶ 27).

Hon. Jesse M. Furman
United States District Judge

Page 4
April 4, 2019

The narcotics sold on the site tended to be sold in individual-use quantities, although some vendors sold in bulk. The offerings for sale on the site at any single time amounted to multi-kilogram quantities of heroin, cocaine, and methamphetamine, as well as distribution quantities of other controlled substances, such as LSD. (*Id.* ¶ 28).

During the course of the investigation, law enforcement seized a wide variety of controlled substances obtained through undercover purchases made on the Silk Road website, including cocaine, crack, heroin, MDMA (commonly known as “ecstasy”), LSD, and oxycodone. (*Id.* ¶ 29).

As noted in the PSR, drugs purchased on Silk Road are linked to real harm, including six overdose deaths, though this defendant is not personally or directly responsible for any of these deaths. (*Id.* ¶ 62).

b. *Counterfeit Identity Documents*

Silk Road also offered for sale counterfeit and fraudulent identity documents, which included, among other things, counterfeit United States and foreign passports, U.S. and foreign drivers’ licenses, and social security cards. As of October 2, 2013, there were approximately 156 different listings for forged identity documents in the “Forgeries” section of the Silk Road website. During the course of the investigation, law enforcement seized counterfeit identity documents that had been ordered through the Silk Road website. (*Id.* ¶ 30).

c. *Computer Hacking Tools and Services*

Silk Road offered a wide variety of computer hacking tools as well as services of computer hackers. As of the takedown of the Silk Road website on October 2, 2013, the following specific computer hacking goods and services (among others) were available on the site:

- Account password hacking tools and services, which included tools for compromising the usernames and passwords of victim electronic accounts, including, among other things, email accounts, Facebook accounts, and other social media accounts. Silk Road also had custom listings made by hackers who offered to compromise email and other electronic accounts on behalf of purchasers.
- Remote Access Tools, commonly known as “RATs,” which allow users to obtain unauthorized remote access to a compromised computer. Once installed, a hacker can use such a tool to view the user’s activity, view the user’s webcam activity, and execute programs remotely, among other things.
- Keyloggers, which allow a user to monitor keystrokes inputted by a victim into his or her computer, used to steal confidential information, including usernames, passwords, or account information.
- Distributed Denial of Service (“DDoS”) services, which involve disabling websites or other publicly available services on the Internet by using large

Hon. Jesse M. Furman
United States District Judge

Page 5
April 4, 2019

networks of compromised computers to flood victim systems with malicious Internet traffic.

(*Id.* ¶ 31).

During the course of the investigation, law enforcement purchased a computer hacking pack from a Silk Road vendor which contained a variety of 50 different computer hacking tools, including RATs, keyloggers, and other computer viruses. The FBI tested a selection of the tools that were purchased from the computer hacking pack, and verified that they operated as advertised to compromise victim computer systems. (*Id.* ¶ 32).

d. *Money Laundering Services*

Silk Road offered a variety of money laundering services to its users, many of which were directly marketed to vendors who sold illegal goods and services on the website as a means to convert proceeds of illegal transactions (obtained in Bitcoins, the required means of payment on the Silk Road website) into other forms of currency. Vendors in this category offered, among other things, the sale of United States currency, anonymous debit cards preloaded with currency, and other prepaid payment systems, including Moneypak cards. (*Id.* ¶ 33).

4. Silk Road's Bitcoin-Based Payment System

The only form of payment accepted on Silk Road was Bitcoins—a decentralized form of electronic currency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through computer software operating on a “peer-to-peer” network. Bitcoin transactions are processed collectively by the computers composing the network. (*Id.* ¶ 34).

All Bitcoin transactions are recorded on a public ledger known as the “Blockchain,” stored on the peer-to-peer network on which the Bitcoin system operates. The Blockchain prevents a user from spending the same Bitcoins more than once. However, the Blockchain only reflects the movement of funds between Bitcoin addresses and therefore cannot by itself be used to determine the identities of the persons involved in the transactions. Only if one knows the identities associated with each Bitcoin address involved in a set of transactions is it possible to meaningfully trace funds through the system. Bitcoins have known legitimate uses, but are also known to be used by cybercriminals for money-laundering purposes, given the ease with which they can be used to move money anonymously. (*Id.* ¶ 36).

Every user on Silk Road had a Silk Road Bitcoin address, or multiple addresses, associated with the user's Silk Road account, where the user could deposit funds into his account. These addresses were stored on “wallet” files maintained on computer servers controlled by Ulbricht. In order to make purchases on the site, the user had to first obtain Bitcoins (typically from a Bitcoin exchanger) and send them to a Bitcoin address associated with the user's Silk Road account. After thus funding his account, the user could then make purchases from Silk Road vendors. When the user purchased an item on Silk Road, the funds needed for the purchase were debited from the user's account and held in escrow (again, in a wallet file maintained by Silk Road) pending

Hon. Jesse M. Furman
United States District Judge

Page 6
April 4, 2019

completion of the transaction. Once the transaction was completed, the Silk Road account of the vendor involved in the transaction was credited with the payment—minus the commission Silk Road took on the sale. The vendor could then withdraw Bitcoins from his Silk Road account by sending them to an outside Bitcoin address, such as the address of a Bitcoin exchanger who would cash out the Bitcoins for real currency. Vendors could also convert Bitcoin proceeds into other forms of currency using various money laundering services offered on the site, as discussed above. (*Id.* ¶ 38).

Silk Road charged a commission for every transaction conducted by its users, generally between 8 to 15 percent. The commission rate varied depending on the size of the sale, *i.e.*, the larger the sale, the lower the commission. Silk Road also used a so-called “tumbler” to process Bitcoin transactions in a manner designed to frustrate the tracking of individual transactions through the Blockchain. According to the Silk Road “wiki” page, Silk Road’s tumbler “sen[t] all payments through a complex, semi-random series of dummy transactions . . . making it nearly impossible to link your payment with any coins leaving the site.” In other words, if a buyer made a payment on Silk Road, the tumbler obscured any link between the buyer’s Bitcoin address and the vendor’s Bitcoin address where the Bitcoins end up—making it fruitless to use the Blockchain to follow the money trail involved in the transaction, even if the buyer’s and vendor’s Bitcoin addresses were both known. (*Id.* ¶ 39).

Silk Road vendors and buyers were required to use the Silk Road Bitcoin-based payment system, or risked being banned from doing business on Silk Road. Specifically, vendors were not permitted to engage with willing customers on the website, but then arrange for payment to occur off the website, thereby avoiding the commissions charged for sales on the site. These kinds of disallowed transactions, referred to as “out of escrow” or “OOE” transactions, were explicitly prohibited by the rules that both vendors and users had to agree to in order to engage in business on the website (explicitly listed in the “Seller’s Guide” and in the agreement that vendors had to consent to when establishing accounts). (*Id.* ¶ 40).

The prohibition on out of escrow transactions was actively enforced by Ulbricht and his administrative staff, including the defendant, Gary Davis. (*Id.* ¶ 41).

5. Volume of Illegal Transactions on Silk Road

The FBI seized computer servers located in Iceland and the United States that were used to operate and back up the Silk Road online marketplace. Those servers included computer databases that contained records for transactions which occurred on Silk Road, during the course of its operation. The transactional database included detailed information regarding each transaction, including the category of product sold, the purchase price (in both Bitcoins and U.S. dollars), and the commission taken by the website (again in both Bitcoins and U.S. dollars). According to that data, between February 2, 2011 and October 2, 2013:

- Approximately 1.5 million transactions occurred over Silk Road, with a total of value of approximately 9.9 million in Bitcoins, which generated commissions of approximately 640,000 in Bitcoins for Silk Road. These transactions had a total value of approximately \$213.9 million in United States currency, and

Hon. Jesse M. Furman
United States District Judge

Page 7
April 4, 2019

generated a total of approximately \$13.2 million in commissions for Silk Road, based on Bitcoin exchange rates at the time that the transactions occurred.

- The vast majority of sales were for illegal narcotics; transactional data indicated that approximately \$183 million of the transactions were categorized as narcotics sales.
- Transactional data from the database indicates the following regarding total sales of heroin, cocaine, methamphetamine and LSD on the Silk Road website during the operation of the website:

	Total Number of Sales	Total Sales Revenue
Heroin	53,649	\$8,930,657
Cocaine	82,582	\$17,386,917
Methamphetamine	34,689	\$8,110,453
LSD	54,567	\$7,073,838

When converted to their marijuana equivalents under the U.S. Sentencing Guidelines, this volume of sales is as follows:

Drug	Quantity (kg)	Marijuana Equivalence per kg	Marijuana Equivalent (kg)
Cocaine	82.6	200	16,520
Heroin	26.8	1,000	26,800
Methamphetamine	8.7	2,000	17,400
TOTAL			60,720 kg

Transactional data extracted from the database indicates the following regarding total sales of counterfeit identity documents:

	Total Number of Sales	Total Sales Revenue
Fake IDs	3,642	\$699,053
Forgeries	3,487	\$197,291
Passports	103	\$105,292

Finally, transactional data from the database indicates the following regarding the total sale of money laundering-related services:

	Total Number of Sales	Total Sales Revenue
Money	14,345	\$2,846,025
Digital Currencies	18,134	\$177,167
Gold	81	\$159,944
Bullion	122	\$80,952
Silver	138	\$9,746

Hon. Jesse M. Furman
United States District Judge

Page 8
April 4, 2019

(*Id.* ¶¶ 42–45).

The database also included information regarding the number of vendors and users on the Silk Road website. According to the information in the database, between approximately January 2011 and October 2013, there were approximately 3,748 different registered vendor accounts, and approximately 115,391 registered buyer accounts who had engaged in at least one transaction on the website. Further, the data indicated a worldwide geographic scope of countries where vendors and buyers indicated that they were located. (*Id.* ¶ 46).

C. Ulbricht's Arrest

On October 1, 2013, Ulbricht was arrested at a Public Library in San Francisco while logged in to the Silk Road acting as “Dread Pirate Roberts.” Specifically, on that date, law enforcement agents observed him enter the library; an undercover agent (“UC-1”), who had successfully infiltrated Ulbricht’s customer support staff, began an online chat with the “Dread Pirate Roberts” and asked him to check a specific message in the support section of Silk Road. After UC-1 confirmed that he was engaged in the conversation with the “Dread Pirate Roberts,” agents arrested Ulbricht and seized his laptop computer, while it was open. At the time of Ulbricht’s arrest, he was logged on to the Silk Road website under the username “Dread Pirate Roberts,” and he was engaged in the online chat with UC-1. (*Id.* ¶ 47).

Subsequent examination of Ulbricht’s computer revealed a significant volume of evidence tying him to the creation, ownership, and operation of Silk Road, as detailed in the PSR. This evidence included, among other things, (1) a spreadsheet listing Ulbricht’s assets, which included a reference to Silk Road being an asset valued at approximately \$104 million as of June 2012;¹ and scanned copies of identification documents belonging to Silk Road staff members, including defendant Gary Davis’s Irish Passport. (*Id.* ¶ 48).

Shortly following Ulbricht’s arrest, law enforcement placed a “banner” on the Silk Road homepage, informing those who visited the website that it had been taken down by the FBI. (*Id.* ¶ 50).

D. Gary Davis's Roles and Responsibilities

From May 2013 through October 2013, the defendant was part of DPR’s small staff of employees who helped run the Silk Road website. The defendant was paid by DPR for his work.²

¹ From a Bitcoin wallet file recovered from Ulbricht’s computer, agents seized approximately 144,341 Bitcoins, which had an approximate value of \$18 million in United States currency at the time that Ulbricht was arrested. (*Id.* ¶ 49).

² Before becoming a site administrator, “Libertas” maintained an account on Silk Road under a different moniker; transactional activity for that moniker reflects that the defendant purchased drugs and anonymous prepaid Visa debit cards from vendors on the Silk Road marketplace, but did not sell drugs on Silk Road. (*Id.* ¶ 53 n.2).

Hon. Jesse M. Furman
United States District Judge

Page 9
April 4, 2019

First, from May to June 2013, the defendant worked as a forum moderator. Forum moderators were responsible for, among other things, monitoring user activity on discussion forums associated with the site, providing guidance to forum users concerning how to conduct business on Silk Road, and reporting any significant problems discussed on the forums to the site administrators and to Ulbricht. Ulbricht paid the defendant for his work as a forum moderator. (*Id.* ¶ 53).

Then, from June until approximately October 2, 2013, the defendant worked as a site administrator. As a site administrator, the defendant's responsibilities included (1) responding to customer support requests from Silk Road users who needed assistance with their buyer or seller accounts on the marketplace; (2) investigating disputes that arose between vendors (*e.g.*, drug dealers) and buyers, including reporting his findings to co-defendant Andrew Michael Jones or to Ulbricht; and (3) helping enforce the rules for doing business on Silk Road, which had been set by Ulbricht. For instance, there was a rule against "out of escrow" sales—*i.e.*, sellers and buyers arranging payments off the site to avoid paying Silk Road commissions. When violations of this rule were discovered, the defendant had the ability to demote a vendor or refer the vendor to "Inigo" (co-defendant Andrew Michael Jones) or to Ulbricht for further discipline. The defendant typically reported such incidents to Jones and occasionally to Ulbricht. Ulbricht paid the defendant \$1,500 per week for his work as a site administrator. (*Id.* ¶ 54).

Davis's Private Message Communications on Silk Road

The following is a selection of the defendant's private message communications on the Silk Road website, as "Libertas":

- On June 7, 2013, "Libertas" sent a private message to a Silk Road user named "Inigo" (*i.e.*, co-defendant Jones), stating: "Hey inigo, I'm on chat but your accounts are offline, as is DPR's. Just wondering if this is a problem on my end or if you both actually are offline? Don't want to be considered as being late for my second day on the job!!"
- On July 14, 2013, "Libertas" sent a private message to "Dread Pirate Roberts," with the subject "Tickets delay," stating: "Hey DPR, Sorry for the CS [customer support] and VS [vendor support] tickets piling up – I logged on last night to clear what was there before I headed out for the night but the site was down for maintenance. . . . I'm pushing down the tickets now but the Opioids category won't be completed by my original ETA. . . . Very sorry about all of that, it's just been an absolutely crazy 24 hours."

(*Id.* ¶ 55).

"Libertas"'s private messages include numerous messages about efforts he made as site administrator to keep the listings of drugs and other items on Silk Road organized under specific categories. For example, on or about July 29, 2013, "Libertas" sent a private message to "DPR" stating:

Hon. Jesse M. Furman
United States District Judge

Page 10
April 4, 2019

I've finished the 'Stimulants' category but I think there'll be a need to revisit it fairly soon. The 'Cocaine' and 'Meth' sub-categories are relatively large, but I'm not entirely sure how I could cut them down any further. I was considering contacting a few of the bestselling vendors in those categories from Vendor Support and asking them if they have any requests they'd like to put forth for consideration on how to better organise their listings, but I wanted to clear it with you first.

'Cocaine' for instance has a 'Crack' sub-category but the other listings are just floating around in the main 'Cocaine' category; as a result, 'crack' listings are mixed in with them. I was going to make a 'Powder' or 'Crystal' category but that's what 'Cocaine' actually describes. I can't cut it down into 'Fishscale' etc. as cocaine quality is an entirely subjective matter and vendors would, for the most part, be listing their products in the highest quality category regardless of the actual quality. 'Meth' could have an 'Ice' subcategory, but again, that's more of a subjective quality matter than anything else and I think it'd be best if I got a general consensus from high-volume vendors in those categories.

Do you think that would be viable?

(*Id.* ¶¶ 55–56). Similarly, on August 4, 2013, “Libertas sent a private message to “DPR” stating:

Hey DPR,

We got a VS ticket in from a vendor wondering if we could open a 'Body armour' category. I presume body armour is permitted as it's not 'weaponry' per se, and I checked with inigo but he couldn't remember whether you said it was permitted or not on the back of a conversation you guys had about it. If it's allowed I'll get him to put it in the 'Apparel' or 'Hardware' category for the time being until I get to sorting out those categories, but I wanted to double-check with you first before giving an answer either way.

I've also created 5 sub categories in Cannabis->Weed:\Blends, High-CBD, Indica dominant, Sativa dominant and Unknown.

It's definitely going to take at *least* a few more days to get everything put into the right categories. When I was selling weed I kept to one or two strains so my exposure to variety was very limited and having to check the genetics and traits of each new strain I come across is really drawing things out given the huge variety out there. Whether a strain is Indica, Sativa or a blend is very rarely stated in the listing description / title, and I don't want to just lump them all into 'Unknown' simply because of my own ignorance when it comes to different strains. 'Unknown' will likely be removed entirely too once I'm finished categorising and have run through that sub-category to determine where each strain would best belong.

As regards an ETA, with this being almost as large a category as 'Prescription' (and with that category taking a veritable age to finish even with less complication due to less product variety) I'd prefer to keep 'Cannabis' as an open-ended 'going concern' for the next couple of days 'til I can get a better idea of roughly how long it's going to take me to get through it. If I give you an ETA now it's highly likely that I'll have to push it back making it somewhat redundant, and I don't want to just say “a week” if I don't think it's necessarily going to take that long.

Hon. Jesse M. Furman
United States District Judge

Page 11
April 4, 2019

(*Id.* ¶ 55).

“Libertas”’s private messages also include “daily notes” that he sent on a regular basis to “Inigo,” summarizing noteworthy actions he had taken or problems he had observed during his shift as site administrator each day. “Inigo” would in turn select which of these actions or issues to report to DPR. For example, on July 11, 2013, “Libertas” sent “Daily Notes” reporting that he had “demoted” the account of a Silk Road vendor named “AfterHour,” noting that the account was “[l]ikely compromised by the police.” As another example, on August 10, 2013, “Libertas” sent “Daily Notes” reporting that he had “demoted” the account of a Silk Road vendor named “jacky” because the vendor had negotiated “deals” on Silk Road “OOE,” or “out of escrow.” (*Id.* ¶ 58).

Davis’s Forum Postings on Silk Road

In addition, the defendant’s forum postings, as “Libertas,” evidence his role as a Silk Road administrator, and his responsibility for responding to customer support questions from Silk Road users in that role. “Libertas”’s forum postings also include postings indicating the need for users to conceal their true identities. For example, in one posting, “Libertas” responded to a user who posted a question on the forum concerning whether it was advisable to activate “scripts”—a setting on his Internet browser—while visiting Silk Road. “Libertas” advised against it, explaining: “Scripts have the potential to take away your anonymity, and if you can easily prevent that from happening, you should.” Similarly, in another posting, “Libertas” responded to a forum posting concerning how to cash out Bitcoins from “Mt. Gox,” a prominent Bitcoin exchanger, without being asked by Mt. Gox to provide verification documents. “Libertas” advised the user not to access Mt. Gox through the Tor network, explaining that “accessing Mt. Gox through Tor will get your account flagged for verification.” (*Id.* ¶ 60).

E. The Defendant’s Involvement in Silk Road’s Successor, Silk Road 2.0

Shortly after law enforcement shut down the original Silk Road in early October 2013, its virtually identical successor—Silk Road 2.0—was launched the following month. Silk Road 2.0 was used by thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to buyers throughout the world, as well as to launder millions of dollars generated by these unlawful transactions. As of September 2014, Silk Road 2.0 was generating sales of at least approximately \$8 million per month and had approximately 150,000 active users. (*See* 14 Mag. 2427, Dkt. 1, ¶¶ 18, 33(d).)

The defendant helped kick-start Silk Road 2.0 by using his credibility with the original Silk Road community to “vouch for” Silk Road 2.0. He posted a link—in an original Silk Road forum, which was still accessible after the website was shut down—by which others could access the new Silk Road 2.0 forums. In addition, for approximately four weeks from November 2013 until his arrest the following month, the defendant served as an administrator for Silk Road 2.0, for which he was paid. He also provided feedback and guidance to the creator of Silk Road 2.0 so that the administrative features of Silk Road 2.0 would more closely resemble those of the original Silk Road. The defendant’s involvement in Silk Road 2.0 ended with his arrest in December 2013. The founder of Silk Road 2.0 was ultimately arrested in November 2014. (PSR ¶ 61).

Hon. Jesse M. Furman
United States District Judge

Page 12
April 4, 2019

II. Procedural History and the Applicable Guidelines Range

The defendant was charged, by Superseding Indictment S1 13 Cr. 950, with three counts: a conspiracy to distribute narcotics (Count One), a computer hacking conspiracy (Count Two), and a money laundering conspiracy (Count Three).³ (Dkt. 3). He was arrested in December 2013 in Ireland. He was originally released on bail in Ireland, but ultimately spent approximately six weeks in custody in Ireland prior to his July 2018 extradition to the United States. He has been detained since his arrival in this District on or about July 13, 2018. (Dkt. 59). On or about October 5, 2018, the defendant pled guilty, pursuant to the Plea Agreement, to a violation of 21 U.S.C. §§ 846 and 841(b)(1)(C), a lesser-included charge of Count One. (Dkt. 71).

The parties, and the U.S. Probation Office, agree that the applicable Guidelines range is 168 to 210 months' imprisonment. (PSR ¶¶ 9 n.1; 88–98, 101 & p. 31; *see also* Def. Mem. 17). Specifically, pursuant to U.S.S.G. § 2D1.1(c)(2), the base offense level is 36, because the conspiracy involved at least approximately 82.6 kilograms of cocaine, 26.8 kilograms of heroin, and 8.7 kilograms of methamphetamine, which converts to a combined drug weight of approximately 60,720 kilograms of marijuana. A two-level enhancement applies, pursuant to U.S.S.G. § 2D1.1(b)(7), because of the distribution of narcotics through mass-marketing by means of a computer. Finally, pursuant to U.S.S.G. §§ 3E1.1(a) and (b), a three-level reduction is warranted for the defendant's timely acceptance of responsibility. The defendant has no criminal history points, producing a total offense level of 35 and a Criminal History Category of I.⁴ (PSR ¶¶ 89, 90, 96, 97).

On February 22, 2019, the Probation Office issued the final PSR. (Dkt. 79). Probation recommends a sentence of 96 months' imprisonment, to be followed by three years of supervised release. (PSR pp. 33–36).

On March 28, 2019, the defense submitted a sentencing letter, seeking a sentence of 30 months' imprisonment. (Dkt. 82) (“Def. Mem.”).

III. Applicable Law

As the Court is well aware, although the United States Sentencing Guidelines are no longer mandatory, they provide strong guidance to courts following *United States v. Booker*, 543 U.S. 220 (2005), and *United States v. Crosby*, 397 F.3d 103 (2d Cir. 2005). Because the Guidelines are “the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions,” *Gall v. United States*, 552 U.S. 38, 46 (2007), district courts must treat the Guidelines as the “starting point and the initial benchmark” in sentencing proceedings. *Id.* at 49. The Guidelines' relevance stems in part from the fact that, while they are advisory, “the sentencing statutes envision both the sentencing judge and the

³ This case was originally assigned to Judge Griesa, but was reassigned to Your Honor in July 2017.

⁴ As the defense correctly notes, the “other arrest” noted in the PSR—from July 13, 2018, the date of the defendant's extradition—is his U.S. arrest in connection with this case. *See* PSR ¶ 104.

Hon. Jesse M. Furman
United States District Judge

Page 13
April 4, 2019

Commission as carrying out the same basic § 3553(a) objectives.” *Rita v. United States*, 551 U.S. 338, 348 (2007). After making that calculation, the Court must consider the seven factors outlined in 18 U.S.C. § 3553(a), which include the nature and circumstances of the offense, the history and characteristics of the defendant, the need to deter criminal conduct and promote respect for the law, the need to protect the public from further crimes of the defendant, and the need to avoid unwarranted sentencing disparities. *Gall*, 552 U.S. at 50 & n.6. If the judge “decides that an outside-Guidelines sentence is warranted, he must consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance.” *Id.*

IV. Discussion

The foregoing sentencing factors weigh in favor of a Guidelines sentence, which would be a significant punishment commensurate with the crime.

First, as to the nature and circumstances of the offense, it is difficult to overstate the seriousness of this offense: The defendant and his co-conspirators operated a massive dark web marketplace that was specifically designed for the purpose of facilitating black-market transactions. The site worked. Until it was taken down by law enforcement, there were more than 1.5 million total transactions, involving more than 100,000 buyer accounts and nearly 4,000 seller accounts. Those transactions had a total value of more than \$210 million in U.S. currency.

Silk Road meaningfully lowered the entry barriers into the underground economy for buyers and sellers alike. It is easy to see why. For sellers, Silk Road provided an anonymous online sales portal, a large customer base, how-to advice from the “Seller’s Guide” and Silk Road discussion forum, and an escrow system enabling sellers to collect payment from customers remotely. Silk Road thus enabled thousands of drug dealers to expand their markets from the sidewalk to cyberspace, and thereby reach countless customers whom they never could have found on the street.

Similarly, for buyers, Silk Road made it simple for anyone anywhere to buy virtually any drug of their choosing. They needed only a computer and a shipping address. With the click of a mouse, a Silk Road user could circumvent all of the physical obstacles that might otherwise prevent or deter one from obtaining drugs locally. Someone who might not know where to find drugs in his or her area, or feel comfortable searching them out, could find and buy drugs effortlessly on Silk Road.

The defendant’s role was important. Given the tremendous growth and scale of Silk Road, Ulbricht could not do everything himself. He relied on a small staff of trusted employees, like the defendant, who worked full-time to ensure the site’s smooth operation. The defendant also helped to enforce the rules Ulbricht set, including the rule against out-of-escrow sales, which ensured that Silk Road received a commission from every sale. Moreover, the defendant worked for Ulbricht over a number of months (May to October, 2013) and, as a general matter, was paid approximately \$1,500 per week.

Second, deterrence interests strongly counsel in favor of a Guidelines sentence. As for general deterrence, the Silk Road was unusually widespread and well-known, as it reached every

Hon. Jesse M. Furman
United States District Judge

Page 14
April 4, 2019

corner of the globe. It was specifically designed to (1) facilitate various kinds of illegal activity on a stunning scale, and (2) make it nearly impossible to determine which individuals, in which locations, were using and operating the site. The Court should send a clear message that those who administer such sites will be met with serious punishment.

Moreover, it is highly unfortunate, but perhaps unsurprising, that Silk Road has spawned a number of similar dark web marketplaces, which continue to pose serious safety concerns and to convert the U.S. mail into a de facto delivery service for narcotics and other contraband. The profitability of such misconduct, unfortunately, appears to continue to appeal to wrongdoers. (From a Bitcoin wallet file recovered from Ulbricht's computer, FBI agents seized approximately 144,341 Bitcoins, which had an approximate value of \$18 million in United States currency at the time that Ulbricht was arrested; today, those same Bitcoins would be worth more than \$700 million.) To the extent that would-be imitators may view the risk of being caught to be low, many are still likely to be deterred if the stakes are sufficiently high.

As for specific deterrence, the defendant's original misconduct—working every day, for several months, to help ensure the smooth operation of a massive drug-dealing enterprise—is extremely serious in its own right. But it is telling—and deeply troubling—that merely a month after Silk Road was shuttered, the defendant joined Silk Road 2.0. Indeed, as noted, he helped kick-start Silk Road 2.0 by using his credibility with the original Silk Road community to “vouch for” Silk Road 2.0, and then served as a paid administrator for Silk Road 2.0. The defendant's astonishing choice to become involved in Silk Road 2.0 supplies the best insight into his decision-making, remorse, and potential for recidivism.⁵ One would hope that the highly publicized arrest of Ulbricht, and the “banner” on Silk Road noting that law enforcement had seized the site, would serve as a clear wake-up call; unfortunately, that was not this defendant's reaction.

Third, considerations of relative culpability also support a Guidelines sentence. The most culpable defendant was Ross Ulbricht, who created and owned Silk Road; he was sentenced to lifetime imprisonment. *See* 14 Cr. 68 (KBF). Ulbricht's right-hand man—who advised Ulbricht on virtually all aspects of Silk Road's operation and managed a staff of computer programmers who helped develop Silk Road's technical infrastructure—was Roger Thomas Clark, who is scheduled for trial before Judge Pauley in May 2020. *See* 15 Cr. 866 (WHP). Below Ulbricht and Clark were a small, trusted staff who helped Ulbricht run the site on a daily basis.

The composition of Ulbricht's customer support staff changed over time, but at the time of Ulbricht's arrest in October 2013, there were only four members of his customer support staff: One was an undercover law enforcement agent, while the other three were the defendants in this case: Andrew Michael Jones, Gary Davis, and Peter Phillip Nash. Jones was another site administrator who served, in several respects, as the defendant's immediate supervisor. Nash was a forum moderator, whose primary roles were (1) keeping the Silk Road discussion forums organized, and (2) serving as Ulbricht's eyes and ears on the discussion forums, monitoring them

⁵ The defendant also appeared to publicly proclaim that he was a hacker, noting on a publicly accessible profile, on a social networking site, that his “likes” included the categories “cyberculture” and “hacking.”

Hon. Jesse M. Furman
United States District Judge

Page 15
April 4, 2019

for any user communications that he thought Ulbricht or the site administrators know about.⁶ For example, if Nash observed any posts by any user whom he suspected of being an undercover law enforcement agent, he would report his suspicions to Ulbricht and the site administrators. Nash would also keep Ulbricht and the site administrators apprised of: any sellers on the forum who were attempting to conduct deals without paying commissions to Silk Road (by arranging their transactions through messages on the forum rather than going through the marketplace payment system); any glitches forum users were reporting with the Silk Road website; any complaints they were making about scams being perpetrated on the website; and any rumors spreading on the forum about “Dread Pirate Roberts” (*i.e.*, Ulbricht) or the Silk Road website. Nash’s Guideline calculation included a three-level reduction for playing a minor role in the offense, as well as a two-level reduction for playing a minor role in a conspiracy involving large quantities of drugs. Nash was ultimately sentenced to approximately 17 months’ imprisonment.

In sum, the defendant is less culpable than Ulbricht and Clark, somewhat less culpable than Jones, but considerably more culpable than Nash.

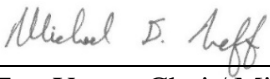
Finally, the defendant’s arguments in favor of leniency (his characteristics, generosity, good deeds, generosity, health considerations/diagnoses, etc.) are certainly legitimate, and should be considered, but pale in comparison to the seriousness of the offense, his role in the offense, and his decision to promptly join Silk Road 2.0.

V. Conclusion

For the reasons set forth above, the Government respectfully submits that a Guidelines sentence would be fair and appropriate in this case.

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York

By: 
Eun Young Choi / Michael Neff / Timothy Howard
Assistant United States Attorneys
(212) 637-2187/2107/2308

cc: Brian E. Klein, Esq. (via ECF)
Marc A. Agnifilo, Esq. (via ECF)
Jacob Kaplan, Esq. (via ECF)

⁶ Nash briefly was promoted to the role of a site administrator in May 2013, but after a few weeks, Ulbricht decided to move him back to the role of forum moderator.